1.   A method of authenticating a transaction, comprising the steps of:

2   connecting a card reader unit to a device having a keypad and display;

initiating a transaction request using the device;

4   communicating the transaction request to a third party through the device; and

receiving a signal at the device to authenticate the transaction.

2.   The method of claim 1, wherein the portable card reader unit is capable of

2   reading a smartcard.

3.   The method of claim 1, wherein the portable card reader unit is capable of

2   reading an optical card.

4.   The method of claim 1, wherein the device is a personal digital assistant

2   (PDA).

5.   The method of claim 1, wherein the device is a telephone.

6.   The method of claim 5, wherein the telephone is a cellular telephone.

7.   The method of claim 1, wherein the signal used to authenticate the

2   transaction is a high-contrast optical signal.

8.   The method of claim 1, wherein the step of communicating the transaction

2   request to a device or third party involves the use of a dual-tone audio signal.

9.   The method of claim 8, wherein the signal is a dual-tone, multi-format

2   (DTMF) signal.

10.   The method of claim 8, wherein the signal is an audio frequency shift

2   keying (AFSK) signal.

11.   The method of claim 8, wherein the signal is a private line (PL) signal.

12.   The method of claim 1, wherein the step of initiating a transaction request

2   at the card reader unit includes the entry of a personal identification number (PIN)

through the keyboard of the device.

13. ₒ   The method of claim 12, wherein the operation of the portable card reader

2   unit is terminated if a PIN entry is attempted more than a predetermined number of times.

14.   The method of claim 1, wherein:

2   the card reader unit further includes a biometric input; and

the step of initiating a transaction request at the card reader unit includes the

4   receipt of biometric data through the biometric input.

5

15.   The method of claim 14, wherein the biometric input is a fingerprint.

16.   The method of claim 1, wherein the transaction request, authentication

2   signal, or both are encrypted.

17.   The method of claim 16, wherein the encryption is based on public-key

2   cryptography.

18.   The method of claim 1, wherein:

2   the card reader or device includes a memory;

the transaction request and authentication signal constitute a session; and

4   information regarding the session is stored in the memory.